UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Related To: JEFFREY WEAVER on behalf of himself and all others similarly situated, Plaintiff, v. WELLTOK, INC., VIRGIN PULSE, INC., COREWELL HEALTH EAST, and PROGRESS SOFTWARE CORPORATION, Defendants.	MDL No. 1:23-md-03083-ADB-PGL **FIRST AMENDED CLASS ACTION COMPLAINT** Civil Action No. 1:24-cv-10645

Plaintiff Jeffrey Weaver ("Plaintiff") individually and on behalf of all similarly situated persons, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, brings this First Amended Class Action Complaint against Defendants Welltok, Inc. ("Welltok"), Virgin Pulse, Inc. ("Virgin Pulse"), Corewell Health East ("Corewell Health"), and Progress Software Corporation ("Progress") (collectively, "Defendants"), and in support thereof allege as follows:

NATURE OF ACTION

1. This First Amended Class Action Complaint is being directly filed into this MDL proceeding pursuant to the Court's MDL Order No. 12.

2. Plaintiff incorporates the allegations contained in the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) in its entirety.

PARTIES

3. Plaintiff Jeffrey Weaver is, and at all times mentioned herein was, an individual and citizen of South Lyon, Michigan. Plaintiff Weaver is a current patient of Corewell Health.

4. Defendant Progress is a software company organized under the laws of Delaware with its principal place of business located at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803. Progress is a public company that produces software for creating and deploying business applications.

5. Defendant Virgin Pulse is a software development company organized under the laws of Delaware with its principal place of business located at 75 Fountain Street, Providence, Rhode Island 02902. On or around November 2023, Virgin Pulse merged with health benefits administrator, HealthComp, and rebranded itself under the name Personify Health, which lists its domestic headquarters at the same address of 75 Fountain Street, Providence, Rhode Island 02902.

6. Defendant Welltok is a software-as-a-service ("Saas") patient engagement company organized under the laws of Delaware with its principal place of business located at 75 Fountain Street, Suite 310, Providence, Rhode Island 02902. Prior to being acquired by Defendant Virgin Pulse in November 2021, Welltok's principal place of business was located at 1515 Arapahoe Street, Tower 3 – Suite 700, Denver, Colorado 80202. Since November 2021, Welltok has been a subsidiary of Defendant Virgin Pulse.

7. Defendant Corewell Heath is a healthcare company based in the State of Michigan, headquartered at 100 Michigan St. NE, Grand Rapids, MI 49503 and operating within three designated regions of Michigan: Southeast Michigan (formerly known as Beaumont Health), Southwest Michigan (formerly known as Spectrum Health Lakeland), and West Michigan (formerly known as Spectrum Health). On October 11, 2022, Beaumont Health and Spectrum Health merged and named the newly formed entity Corewell Health.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000) and is a class action in which one or more class members are citizens of states different from Defendants.

9. Absent the Court's MDL Order No. 12 (Direct Filing Order), Plaintiff would have otherwise filed the case in each district court noted below, with the following bases:

a. Plaintiff Weaver would have filed his action in the United States District Court, Eastern District of Michigan, which has personal jurisdiction over Defendants Welltok, Virgin Pulse, Progress, and Corewell Health, because those Defendants and their affiliates do business in the State of Michigan and the claims asserted herein arise from conduct occurring in Michigan. The Eastern District of Michigan is the proper venue for this action pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in that District and those Defendants have harmed Class Members residing in that District. Further, Corewell Health is headquartered in that District.

FACTUAL ALLEGATIONS

Nature of Defendants' Businesses

10. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Plaintiff's and millions of other similarly situated clients', patients', and/or employees' Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (collectively, "Private Information" or "PI") from cybercriminals who obtained such Private Information through the MOVEit Transfer tool server in May 2023 (the "Data Breach").

11. According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[1] PHI is deemed private under the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§ 1320d, et seq., as well as multiple state statutes. According to the U.S. Department of Health & Human Services ("HHS"), PHI "is information, including demographic data," that relates to: "the individual's past, present or future physical or mental health or condition," "the provision of health care to the individual," or "the past, present, or future payment for the provision of health care to the individual," and that "identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual." Individually identifiable health information includes many common identifiers (*e.g.*, name, address, birth date, SSN)."[2]

12. As used throughout this Complaint and previously defined in paragraphs 10-11, "Private Information" is further defined as all information exposed by the Data Breach, including

---

[1] *See Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED)* at 3, n.3, FTC (June 2019), https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf.

[2] *See Summary of the HIPAA Privacy Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited June 5, 2024).

all or any part or combination of name, address, birth date, SSN, PHI, driver's license information (including license number, state, home address, dates of issuance or expiration), telephone number, email address, tax identification number, credit card number, or dispute documents with PII (such as images of government-issued identifications).

13. The factual allegations relating to Progress's business and its MOVEit software, as well as the underlying Data Breach, are contained in the Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) in its entirety.

14. Defendant Virgin Pulse is a software development company which touts itself as the leading global provider of tech-enabled solutions focused on improving the health and wellbeing of its members. On its website, Virgin Pulse claims to be "Trusted by Leading Organizations Everywhere," including 7,000+ organizations, 25% of which are part of the Global Fortune 500, in 190 countries and territories worldwide.[3]

15. On November 10, 2021, Virgin Pulse issued a press release, announcing that it had completed its acquisition of Welltok, which stated that "[c]ombining Welltok's activation engine with Virgin Pulse's daily engagement platform will drive better health outcomes and cost reductions for the companies' 4,100 global employer, health plan and health system clients."[4] According to Virgin Pulse, "[w]ith this acquisition, Virgin Pulse will introduce the industry's first end-to-end engagement and activation platform that supports clients, members, and consumers across the entire health continuum by," among other things, "[l]everaging the industry's most comprehensive consumer database for 275 million lives." *Id.*

---

[3] *Homepage*, Virgin Pulse, https://international.virginpulse.com/ (last visited June 5, 2024).

[4] *Virgin Pulse completes acquisition of Welltok, expanding health engagement capabilities for employers, payers and health systems*, Virgin Pulse, https://international.virginpulse.com/press-releases/virgin-pulse-completes-acquisition-of-welltok-expanding-health-engagement-capabilities-for-employers-payers-and-health-systems/

16. On or around November 2023, Virgin Pulse merger with HealthComp, an independent, tech-enabled health plan benefits administrator and payment integrity provider, supporting self-insured organizations by, among other things, helping them design cost-effective employee benefits strategies. On or around February 2024, the combined entity rebranded itself as "Personify Health" "According to Personify Health's CEO, Chris Michalak, former CEO of Virgin Pulse, "Personify Health aligns very well with where we're going as a company. We talked about launching a personalized health platform and that's going to be the foundation of what we bring to clients in the market," Michalak said. "This is a platform that they can customize to the needs of their population, as well as a platform that works for their members, a customized experience for each and every member wherever they are in their healthcare journey. Personify captures the essence of what we're trying to be and how we're trying to distinguish our company from others in the healthcare space."[5] As a rebranded entity, Virgin Pulse now works with 1,000 self-insured employers and has 7,500 overall clients including through health plan partnerships, serving more than 18 million members. The rebranded entity is valued at approximately $3 billion.[6]

17. Personify Health's website provides access to Virgin Pulse members to log into the "Virgin Pulse member login" and Virgin Pulse member support" platforms.[7] Additionally, Personify Health's Terms of Use identifies Virgin Pulse as the party to that agreement and states that "Virgin Pulse ("Virgin Pulse " or "we", "us", "our"), provides access to our Web site located at www.virginpulse.com (the "Site"), subject to your acceptance of these Terms of Web site Use ("Terms")."[8]

---

[5]https://www.fiercehealthcare.com/health-tech/virgin-pulse-healthcomp-rebrand-personify-health-employer-health-company-eyes-double

[6] *Id.*

[7] https://personifyhealth.com/company/locations/

[8] Terms of Use - Personify Health (last visited June 7, 2024).

18. Defendant Welltok is a data-driven patient engagement company that utilizes a single platform to connect healthcare providers with patients by providing personalized, consumer-facing healthcare content and technology, including patient-communications services. By delivering personalized resources to individuals, Welltok's platform helps individuals take critical actions such as scheduling a doctor's appointment, selecting insurance coverage, or refilling medications. Welltok's platform maintains a massive consumer database that stores and transfers the Private Information of its healthcare patients, clients, and employees using the MOVEit Transfer tool.

19. More than 100 healthcare providers, health plans, employers, and pharmacies contracted with Welltok as a vendor to run patient engagement and acquisition campaigns and store their patients' Private Information on Welltok's platform, including, but not limited to, (collectively, Welltok's "Clients"):

- Aetna
- Adventist Healthcare
- Altru
- Asuris Northwest Health
- Anthem Blue Cross and Blue Shield
- Arkansas Blue Cross and Blue Shield
- Baylor Scott & White Health
- Baxter International Inc. and Subsidiaries Welfare Benefit Plan
- BridgeSpan Health
- Blue Cross and Blue Shield of Massachusetts
- Blue Cross and Blue Shield of Minnesota and Blue Plus
- Blue Cross and Blue Shield of Alabama
- Blue Cross and Blue Shield of Kansas
- Blue Cross and Blue Shield of North Carolina
- Blue Cross Blue Shield of Illinois
- Blue Cross Blue Shield of Texas
- Blue Cross Blue Shield of New Mexico
- Blue Cross Blue Shield of Oklahoma
- Blue Cross Blue Shield of Montana
- Blue Cross Blue Shield of Massachusetts.
- Blue Cross and Blue Shield of Kansas

- Blue Cross and Blue Shield of Kansas City
- Blue Cross of Idaho Health Service, Inc.
- Blue Cross Blue Shield of Massachusetts
- BlueCross & BlueShield of Minnesota
- Blue Cross & Blue Shield of Mississippi, A Mutual Insurance Company
- Blue Cross and Blue Shield of North Carolina
- Blue Cross Blue Shield of North Dakota
- Blue Cross and Blue Shield of Nebraska
- Blue Cross & Blue Shield of Rhode Island
- Blue Cross Blue Shield of South Carolina
- BlueCross BlueShield of Tennessee
- Blue Cross and Blue Shield of Vermont
- Blue Cross Blue Shield of Wyoming
- Blue Cross and Blue Shield of Arizona, Inc.
- Blue Shield of California
- Blue Shield of California OR Blue Shield of California Promise Health Plan
- Capital Blue Cross
- CareFirst of Maryland, Inc. dba CareFirst BlueCross BlueShield
- Centerwell Pharmacy
- CHI Health – NE
- CHI Memorial – TN
- CHI Memorial – GA
- CHI Mercy Health
- CHI St. Joseph Health
- CHI St. Luke's Health Brazosport
- CHI St. Luke's Health Memorial
- CHI St. Vincent
- Community Health Network
- Community Health Group
- Ella EM Brown Charitable Circle dba Oaklawn Hospital
- EmblemHealth Plan, Inc.
- EmblemHealth Insurance Company
- Evoqua Water Technologies
- Excellus Health Plan, Inc.
- Faith Regional Health Services
- Florida Blue
- Freedom Health, Inc.
- Group Hospitalization and Medical Services Inc., dba CareFirst BlueCross BlueShield
- Hawaii Medical Service Association
- Health First Shared Services, Inc
- Health Insurance Plan of Greater New York
- Highmark Inc.,
- Highmark Inc.

- Highmark Western and Northeastern New York
- Highmark Delaware
- Highmark West Virginia
- Highmark Blue Cross Blue Shield Delaware
- Highmark Blue Cross Blue Shield West Virginia
- Highmark Blue Cross Blue Shield of Western New York
- Highmark Blue Shield Northeastern New York
- Holzer Health System
- Horizon Blue Cross Blue Shield of New Jersey
- Hospital & Medical Foundation of Paris, Inc. dba Horizon Health
- Humana Inc.
- Independence Blue Cross
- Johns Hopkins Health Plans
- Louisiana Health Service & Indemnity Company d/b/a Blue Cross and Blue Shield of Louisiana
- Marshfield Clinic Health System
- Mass General Brigham Health Plan
- MetroPlus Health Plan
- Mercy Med Ctr Des Moines-IA
- MercyOne Newton Med Ctr-IA (Skiff)
- Mercy Med Ctr W Lakes Des Moines-IA
- Mercy Med Ctr Centerville-IA
- MercyOne IA Heart Des Moines-IA
- Optum Specialty Pharmacy
- Optum OrthoNet
- Optum AppleCare Medical Group
- Optimum HealthCare, Inc.
- OSF Healthcare
- Pinellas County Sherriff's Office
- Premier Health
- Priority Health
- Premera Blue Cross
- Regence BlueCross BlueShield of Oregon
- Regence BlueShield
- Regence BlueCross BlueShield of Utah
- Regence Blue Shield of Idaho
- St. Alexius Health
- St Anthony Hospital
- St. Bernards Healthcare
- St Joseph Health
- St. Luke's Health
- Sutter Health
- ThedaCare, Inc.
- Taylor Farms

- United Regional Health Care System
- United Healthcare Services, Inc.
- Trane Technologies Company LLC and/or group health plans sponsored by Trane Technologies Company LLC or Trane U.S. Inc.
- Triple-S Salud, Inc.
- Trinity Health System
- The group health plans of Stanford Health Care, of Stanford Health Care, Lucile Packard Children's Hospital Stanford, Stanford Health Care Tri-Valley, Stanford Medicine Partners, and Packard Children's Health Alliance
- The Guthrie Clinic
- Virginia Mason Franciscan Health
- West Virginia University Health System
- Wellmark Advantage: Blue Cross Blue Shield Of Michigan
- Wellmark, Inc., d/b/a Wellmark Blue Cross and Blue Shield of Iowa, and Wellmark of South Dakota, Inc. d/b/a Wellmark Blue Cross and Blue Shield of South Dakota
- Wipro Medical
- Yale New Haven Health

20. Defendant Corewell Heath operates the largest healthcare system in the state of Michigan, providing patients with a variety of healthcare services, such as using its website to locate doctors, schedule appointments, and pay medical bills. According to its website, Corewell Health has 1.3+ million health plan members, 9,000+ employers contracted by Priority Health (a subsidiary health plan), 65,000+ team members, 12,000+ affiliated, independent, and employed physicians and advanced practice providers, 15,000+ nurses, 21 hospital facilities, and 300+ ambulatory/outpatient locations. Corewell Health's facilities include hospitals, nursing homes, urgent care centers, our medical staff, home health care agencies, hospices, clinics, and offices.

Defendants Collected, Stored, and were Responsible for Protecting Plaintiff's and Class Members' Private Information.

21. As a condition to obtain healthcare services and/or employment from Welltok's Clients, such as Corewell Health, Plaintiff and Class Members were required to give their sensitive and confidential Private Information, directly or indirectly, to Welltok's Clients.

22. Unbeknownst to Plaintiff and Class Members, Welltok's Clients, in turn, provided

Welltok with access to that Private Information, directly or indirectly, to collect, store, and transfer using Welltok's platform that utilized MOVEit software. For example, Corewell Health collected, stored, and transferred Plaintiff Weaver's PII and PHI in connection with services provided to him by Corewell Health. Corewell Health provided Welltok with access to that PII and PHI by causing such information to be used, stored, and transferred to Welltok's contact platform, which utilized the MOVEit Transfer tool. According to the Data Breach Notice Letters that Plaintiff Weaver received from Welltok, "Welltok software operates a contact platform for Corewell Health and received your information in connection with those services."

23. By obtaining, collecting, storing, and sharing Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

24. Defendants made explicit promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information. Notably, in their respective Privacy Notices and Privacy Policies, Defendants claim that the privacy of individuals' PII and PHI is a top priority and pledge a commitment to protecting that information from unauthorized use, including by using "state of the art care" and "the latest technologies" to ensure the utmost security in doing so.

25. For example, Virgin Pulse's General Privacy Notice (updated as of September 15, 2023) pledges that "[w]e are committed to protecting your rights and your privacy. To ensure data security, We follow reasonable physical, electronic and managerial procedures designed to safeguard and secure your data and Personal Information."[9] With respect to the transfer of its healthcare clients' and patients' personal information to authorized parties, Virgin Pulse represents

[9] Privacy Notice - Virgin Pulse | Virgin Pulse

that "[w]hen we receive Personal Information from a third party, or share Personal Information with a third party, we execute appropriate written agreements based on the applicable jurisdiction."[10] Virgin Pulse's privacy policy "applies to all Personal Information whether collected online or offline" and warns users that "if you choose to withhold some Personal Information, We may be unable to provide you with certain services."[11]

26. According to its Privacy Notice, Virgin Pulse collects, stores, and transfers "any information, including personal and material circumstances, that allows a person to become identifiable[,]" including, but not limited to:

- Your email address;
- Your profile information, including your profile photo;
- Your gender, date of birth and age;
- Your social security number or employee identification number;
- Biometric information such as your blood pressure or weight;
- Information about your health;
- Information about your fitness and related wellness activities offered within the Program;
- Information about your participation and performance in the Program and related challenges;
- Information you voluntarily share about yourself during any calls you participate in with Our health coaches;
- Information you voluntarily share with Our Member Services team;
- The comments and contributions you may make on the web-based platform or mobile application; and
- Additional information you may provide as you submit queries and requests to Us.

27. In addition, on its website, Virgin Pulse maintains an "Authorization For Use and Disclosure of Protected Health Information" (the "Authorization"), which "pertains to your right to the privacy of your Protected Health Information (PHI)."[12] The Authorization promises that:

> Your PHI, including health screening results, health assessment responses and coaching notes, will not be obtained by your Program Sponsor except as described

[10] *Id.*
[11] *Id.*
[12] https://www.virginpulse.com/gina-phi-notice/ (last acc. on May 20, 2024).

> in this Authorization and will not be used by your Program Sponsor for any employment-related purposes. Your PHI will not be sold, exchanged, transferred or otherwise disclosed to third parties for commercial purposes. **Your PHI will not be disclosed except as permitted by this Authorization or Our Privacy Notice, or to the extent permitted by law.** You will not be asked or required to waive the confidentiality of your PHI as a condition of participating in Our Program or receiving an incentive. You may not be discriminated against in employment because of the PHI you provide as part of participating in the wellness program, nor may you be subjected to retaliation if you choose not to participate.
>
> **We will only share your PHI with entities that have a legal right to access it**, that are obligated to protect it in similar ways that we are obligated to protect it, and that assist in providing Our Program or other health benefits to you…[13]

28. Similarly, Welltok's General Privacy Notice (effective September 30, 2020), claims that "[p]rotecting your personal data is important to Welltok and its subsidiaries."[14] Welltok's LinkedIn page also represents that its software platform is a "single, **secure** platform."[15]

29. According to its Privacy Notice, Welltok obtains PII and PHI as follows:

> When you use any of our websites or mobile applications (the "Platform") or use our and our engagement/customer relationship management platforms and services ("CRM"), we may collect information about you, including information that can be used to identify you ("Personal Information").
>
> Additionally, we may collect Personal Information from your health plan, your employer's self-funded health plan, your employer, a health service provider, your pharmacy and/or other similar types of entities (your "Sponsor") or from other third parties described in this Privacy Notice.[16]

30. According to its Privacy Notice, the type of personal information that Welltok collects, stores, and transfers includes, but is not limited to:

- Social Security number;
- Name;
- Date of birth;
- Email address;
- Home address;

[13] *Id.* (Emphasis added)
[14] *See* Exhibit A attached hereto.
[15] https://www.linkedin.com/company/welltok-inc-/ (emphasis added) (last visited June 7, 2024).
[16] *See* Ex. A.

- Business address;
- Phone number;
- Other identification numbers (e.g. state-issued identification number, member number, or employee number);
- Geolocation Data; and
- Biometric Information.

31. Welltok states that it "may also collect PHI as defined under the Health Insurance Portability and Accountability Act ("HIPAA"), which is a regulated subset of Personal Information. We collect this data to provide you with the services and functionality that you request (the "Services"), as well as for the other purposes described in this Privacy Notice." *Id.* Specific types of PHI collected by Welltok cited in its Privacy Notice include "claims information, lab and biometric information, electronic medical records/electronic health records, and program activity." *Id.* Additional types of personal information specifically related to individuals' health that Welltok collects, stores, and transfers includes, but is not limited to:

- Physical Activity and Movement Data;
- Health Risk Assessments;
- Lab Scores;
- Data Related to Managed Health Programs;
- Medications and Prescriptions;
- Cognitive Assessment Data;
- Health Conditions or Diseases;
- Health Plan Information;
- Insurance Information; and
- Eating Habits and Nutrition.

32. As Welltok's Policy Notice promises, "[w]e may provide your PHI to a Sponsor, Connect Partner or third-party service provider as either a covered entity or a business associate. We will only disclose your PHI as allowed under HIPAA to provide you with the Services or with your express consent." *Id.*

33. Corewell Health's Notice of Privacy Practices, which all Corewell Health facilities are required to follow, asserts that "[w]e are committed to your privacy" and that "[t]he privacy of

your health information has always been a priority at Corewell Health."[17] In that Notice, Corewell Health makes a "Pledge Regarding Your Health Information," stating that "[w]e understand that your health information is personal, and we are committed to protecting it." The Notice notes that Corewell Health's pledge to protect privacy rights is an "ongoing commitment." According to the Notice, the information collected and stored by Corewell Health includes both physical and mental health care information.

34. Corewell Health also maintains a Privacy Policy that "sets forth the guidelines used for protecting the information you…provide during visits to https://corewellhealth.org."[18] The type of information collected and stored by Corewell Health from patients and users includes their personal information provided to participants in Corewell Health's healthcare network, the content of their email communications with Corewell Health, together with their email addresses and Corwell Health's responses thereto, and their website use information as they browse Corewell Health's website.

35. In the first paragraph of its Privacy Policy, Corewell Health promises that "[w]e will not sell, share, or rent this information to others in ways different from what is disclosed in this statement." The ways disclosed in the Privacy Policy include "shar[ing] the information we collect with agents, contractors or affiliates of ours for the purpose of providing services to us." *Id.* The Privacy Policy also reserves the right to release collecting personal information when necessary to "comply with the law, other agreements, or to protect the rights, property, or safety of [https://corewellhealth.org], its owners or others."

36. Corewell Health also has a MyChart Privacy Policy concerning the private

[17] *See* Notice of Privacy Practices (Patient Privacy) | Corewell Health (spectrumhealth.org)
[18] *See* Privacy Policy | Corewell Health

information collected and stored on Corewell Health's "MyChart" mobile application and website. In that Privacy Policy, Corewell Health states that "[t]he importance of security for all personal information including, but not limited to, health information associated with you, is of utmost concern to us. Through MyChart, we exercise state of the art care in providing secure transmission of your information from your computer or mobile device to our servers. Information collected by the MyChart site and app is stored in secure operation environments that are not available or accessible to the public."[19] Corewell Health further assures patients that "MyChart is not only HIPAA compliant but additionally utilizes the latest technologies to ensure utmost security."

37. The tools, features, and services available through MyChart include "access to your medical record information, (2) access to information in your Priority Health account (if you have one), and (3) connection to participating physicians and other licensed health care professionals ("Providers") in real time, via live video, telephone and/or secure email, for the diagnosis and treatment of patients over the Internet." *Id.* The MyChart Privacy Policy assures that Corewell Health "will not sell, share, or rent this information to others except: (i) when you've provided your prior consent; or (ii) as disclosed in this Policy." The private information collected and stored by MyChart includes patients' medical records, the results of certain medical tests, claims summaries, as well as information that Corwell Health specifically requests from users when they:

- Sign up for MyChart;
- Provide preferred pharmacy locations;
- Provide self-reported remedies, supplements and over-the-counter medications;
- Provide self-reported immunizations;
- Send a secure message to your health care provider, billing office or MyChart customer support;
- Request an appointment or health service(s);
- Access test results;

[19] *See* Privacy Policy | Corewell Health

- Connect and communicate with physicians or other licensed health care professionals ("Providers") in real time, via live streaming video, telephone and/or secure email for the purpose of diagnosis and/or treatment ('eCareServices');
- Use the Abriiz tool to record information about your health and wellness;
- Request access or grant access to your account for another MyChart account user.

38. None of Defendants' respective Privacy Notices or Privacy Policies permitted any Defendant to share or disclose Plaintiff's and Class Members' PII or PHI to unauthorized third parties as occurred in the Data Breach.

Defendants Failed to Protect Plaintiff's and Class Members' Private Information

39. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendants to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

40. Defendants had duties to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to unauthorized third parties, and Welltok had a duty to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendants have a legal duty to keep consumer's Private Information safe and confidential.

41. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members or by Welltok exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

Defendants Failed to Comply with FTC Guidelines

42. The Federal Trade Commission ("FTC") has promulgated numerous guides for

businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

43. In October 2016, the FTC updated its publication, Protecting Private Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

44. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

45. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

46. These FTC enforcement actions include actions against administrative services companies and software companies, like Defendants.

47. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices, and Welltok failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

48. Defendants were at all times fully aware of their obligations to protect the Private Information of the patients and employees in their networks yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Welltok, Virgin Pulse, and Corewell Health Failed to Comply with HIPAA Guidelines

49. Welltok, Virgin Pulse, and Corewell Health are each a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

50. Welltok, Virgin Pulse, and Corewell Health are covered entities under HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable

Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

51. Covered entities are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[20] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

52. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

53. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

54. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

55. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

56. HIPAA's Security Rule requires covered entities and business associates to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

[20] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

57. HIPAA also requires covered entities and business associates to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, covered entities and business associates are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

58. HIPAA and HITECH also obligate covered entities and business associates to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

59. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires covered entities and business associates to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[21]

[21] *Breach Notification Rule*, U.S. Dep't. of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last updated July 26, 2013).

60. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

61. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

62. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[22] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says: "represent the industry standard for good business practices with respect to standards for securing e-PHI."[23]

Defendants Failed to Comply with Industry Standards

[22] *Security Rule Guidance Material*, U.S. Dep't. of Health & Human Servs., http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html. (last updated Feb. 16, 2024).

[23] *Guidance on Risk Analysis*, U.S. Dep't. of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last updated July 22, 2019).

63. As noted above, experts studying cybersecurity routinely identify administrative services companies and software companies as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

64. Some industry best practices that should be implemented by administrative services companies and software companies dealing with sensitive Private Information, like Defendants, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

65. Other best cybersecurity practices that are standard in the administrative services and software industries include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

66. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (“”), which are all established standards in reasonable cybersecurity readiness.

67. Defendants failed to comply with these accepted standards in the administrative

services and software industries, thereby permitting the Data Breach to occur.

Defendants Breached Their Duties to Safeguard Plaintiff's and the Class's Private Information

68. In addition to their obligations under federal and state laws, Defendants owed duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed duties to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the Private Information of Class Members.

69. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data, and Welltok failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect Plaintiff's, clients', patients', and employees' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to sufficiently train their employees and vendors regarding the proper handling of Plaintiff's, clients', patients', and employees' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and,

g. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

70. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access their computer networks and systems which contained unsecured and unencrypted Private Information.

71. Had Defendants remedied the deficiencies in their information storage and security systems or those of their vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

Common Injuries & Damages

72. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) general damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for

unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

The Data Breach Increases Victims' Risk Of Identity Theft

73. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

74. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. As a result of the Data Breach, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

75. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

76. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity–or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

77. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a

victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

78. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[24]

79. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

80. The development of "Fullz" packages means here that the stolen Private Information from the data breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not

[24] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sept. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/

be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

81. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

82. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

83. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

84. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

85. Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

86. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank

accounts, credit cards, driving records, tax and employment histories and other private information increases."[25] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[26]

87. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[27]

88. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[28] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[29]

89. The California state government warns consumers that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you

---

[25] *See Avoid Identify Theft: Protect Social Security Numbers*, Soc. Sec. Admin. https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases (last visited June 5, 2024).

[26] *Id.*

[27] *Identity Theft and Your Social Security Number*, Soc. Sec. Admin., https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 5, 2024).

[28] *See How to Protect Yourself from Social Security Number Identify Theft*, Equifax, https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last visited June 5, 2024).

[29] *See* Julia Kagan, *What Is an SSN? Facts to Know About Social Security Numbers* (Feb. 15, 2024), https://www.investopedia.com/terms/s/ssn.asp.

retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[30]

90. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraudulent activity to obtain a new number.

91. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[31]

92. Thus, due to the actual and imminent risk of identity theft, Welltok, in its Notice Letters, instructs Plaintiff and Class Members to take the following measures to protect themselves against the misuse of their Private Information:

> We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information*. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. While Welltok will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are included in this letter.

[30] *See Your Social Security Number: Controlling the Key to Identity Theft*, State of Cali. Dep't of Justice, https://oag.ca.gov/idtheft/facts/your-ssn (last visited June 5, 2024).
[31] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft

93. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter as well as monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

94. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[32]

95. These efforts are also consistent with the FTC's recommendations that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[33]

96. And for those Class Members who experience actual identity theft and fraud, the GAO Report also noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[34]

[32] *See* United States Government Accountability Office, GAO-07-737, Private Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[33] *See Identity Theft.gov*, FTC, https://www.identitytheft.gov/Steps (last visited June 5, 2024).
[34] *See* GAO Report, *supra* note 27.

Diminution Value Of Private Information

97. PII and PHI are valuable property rights.[35] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

98. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[36]

99. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[37]

100. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[38]

101. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[39]

102. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and

---

[35] *See, e.g.,* Randall T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[36] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak* (Nov. 5, 2019, 5:00 AM PST), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[37] *The personal data revolution*, Datacoup, https://datacoup.com/ (last visited June 5, 2024).

[38] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited June 5, 2024).

[39] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

103. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[40]

104. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

105. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[41] Indeed, during 2019 alone, over 41 million healthcare records were exposed,

---

[40] *Medical I.D. Theft*, EFraudPrevention, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last visited June 5, 2024).

[41] Adil Hussain Seh, *et al*, *Healthcare Data Breaches: Insights and Implications*, Nat'l Lib. Of Med. (May 13, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/.

stolen, or unlawfully disclosed in 505 data breaches.[42] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.

106. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[43]

107. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[44] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.

108. According to account monitoring company LogDog, medical data sells for $50 and up on the dark web.[45]

109. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information

---

[42] Steve Alder, *December 2019 Healthcare Data Breach Report*, The HIPAA J. (Jan. 21, 2020), https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.
[43] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.
[44] *See* Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.
[45] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content

compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., names, dates of birth, PHI, and Social Security numbers.

110. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

111. The fraudulent activity resulting from the Data Breach may not come to light for years.

112. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

113. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' networks, amounting to more than eight million individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

114. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Cost of Credit & Identity Theft Monitoring is Reasonable and Necessary

115. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private

Information for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

116. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

117. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

118. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

Loss Of The Benefit Of The Bargain

119. Furthermore, Defendants' poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to obtain healthcare services and/or accept employment from Welltok's Clients, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for, or being paid less for, the necessary data security to protect the Private Information, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received healthcare services, health plan benefits, and/or employment positions that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Welltok's Clients.

Plaintiff's Specific Experiences and Harm

Plaintiff Jeffrey Weaver

120. Plaintiff Weaver is a current patient at Corwell Health, which, according to Plaintiff Weaver's Notice Letter, contracted with Welltok to "operate[] a contact platform for Corewell Health East and received [Plaintiff Weaver's] [Private Information] in connection with those services."

121. In order to obtain healthcare services at Corewell Health, Plaintiff Weaver was required to provide his Private Information, directly or indirectly, to Defendants, including his name, date of birth, health insurance information, Social Security number, and other sensitive information.

122. At the time of the Data Breach—in or around May 2023—Defendants retained Plaintiff Weaver's Private Information in their systems.

123. Plaintiff Weaver is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. He would not have entrusted his Private Information to Defendants had she known of Defendants' lax data security policies.

124. Plaintiff Weaver received a Notice Letter by U.S. mail addressed to his directly from Welltok, writing on behalf of Corewell Health, dated November 17, 2023. According to the Notice Letter, Plaintiff Weaver's Private Information was improperly accessed and obtained by unauthorized third parties, including his "name, date of birth, email address, phone number, diagnosis, health insurance information, and Social Security Number."

125. Although the Notice Letter disclosed that on July 26, 2023, Welltok had been

"alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," it took Welltok four months to notify Plaintiff Weaver and other Class Members of the Data Breach's occurrence after being notified of the cyberattack by Progress. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again have not been explained or clarified to Plaintiff Weaver and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

126. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

127. As a result of the Data Breach, and at the direction of the Notice Letter, Plaintiff Weaver has spent significant time on making reasonable efforts to mitigate the impact of the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Specifically, in response to the Data Breach, Plaintiff Weaver has spent substantial time on mitigation efforts, including but not limited, to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, enrolling in credit monitoring service after the Data Breach, and monitoring his financial accounts for any indication of additional fraudulent activity, which may take years to detect.

128. Plaintiff Weaver suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data

Breach.

129. Plaintiff Weaver suffered additional injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) general damages; and (x) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

130. Moreover, the Data Breach has caused Plaintiff Weaver to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

131. As a result of the Data Breach, Plaintiff Weaver is at present risk and will continue to be at increased risk of identity theft and fraudulent activity for years to come.

132. As a result of the Data Breach, Plaintiff Weaver anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm already caused and continue to be caused by the Data Breach.

133. Plaintiff Weaver has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

134. Plaintiff brings this action on behalf of themselves and the following classes:

(1) Progress Nationwide Class: All persons whose Private Information was compromised in the MOVEit data breach.

(a) Progress Michigan Class: All residents of Michigan whose Private Information was compromised in the MOVEit data breach.

The foregoing state-specific Progress class is referred to as the "Progress State Class."

(2) Welltok Nationwide Class: All persons whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by Welltok.

(a) Welltok Michigan Class: All residents of Michigan whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by Welltok.

The foregoing state-specific Welltok class is referred to as the "Welltok State Class."

(3) Virgin Pulse Nationwide Class: All persons whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by Virgin Pulse.

(a) Virgin Pulse Michigan Class: All residents of Michigan whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by Welltok.

The foregoing state-specific Virgin Pulse class is referred to as the "Virgin Pulse State Class."

(4) Corewell Health Nationwide Class: All persons whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by Corwell Health.

(a) Corewell Health Michigan Class: All residents of Michigan whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by Corwell Health.

The foregoing state-specific Corwell Health class is referred to as the "Corwell Health State Class."

135. The Progress, Welltok, Virgin Pulse, and Corwell Health Nationwide Classes are collectively referred to as the "Nationwide Classes." Excluded from the Class are: (1) the judges

presiding over the action; (2) the Defendants, their subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

136. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

137. **Numerosity**: Class members are so numerous that their individual joinder is impracticable, as the proposed Class includes at least tens of millions of members who are geographically dispersed.

138. **Typicality**: Plaintiff's claims are typical of Class Members' claims. Plaintiff and all Class Members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the Class Members he seeks to represent.

139. **Adequacy**: Plaintiff's interests are aligned with the Class they seek to represent and Plaintiff have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and his counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and undersigned counsel.

140. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendants' wrongdoing. Even if Class v could afford such individual litigation, the court system could not. Individualized

litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

141. **Commonality and Predominance:** The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII and PHI from unauthorized access and disclosure;

b. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII and PHI;

c. Whether Defendants breached their duties to protect Plaintiff's and Class Members' PII and PHI;

d. Whether Defendants violated the statutes alleged herein;

e. Whether Plaintiff's and all other Class Members are entitled to damages and the measure of such damages and relief.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF
NEGLIGENCE

(Brought by Plaintiff Weaver on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes [alternatively, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes] against Progress, Welltok, Virgin Pulse, and Corewell Health)

142. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if

fully set forth herein.

143. Plaintiff brings this claim against Progress, Welltok, Virgin Pulse, and Corewell Health on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes or, in the alternative, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes.

144. Defendant Corewell Health, like Welltok's other Clients, requires its patients, plan members, customers, users, and/or employees, including Plaintiff and Class Members, to submit non-public Private Information to Defendants in the ordinary course of providing from services. Corewell Health and Welltok's other Clients collected and stored the Private Information of Plaintiff and Class Members during the course of providing services to Plaintiff and Class Members.

145. Corewell Health and Welltok's other Clients collected, stored, and shared the Private Information of Plaintiff and Class Members with Welltok and Virgin Pulse in connection with the services provided by Welltok and Virgin Pulse to Corewell Health and Welltok's other Clients.

146. Plaintiff and Class Members entrusted Defendants, directly or indirectly, with their Private Information with the understanding that Defendants would safeguard their information from unauthorized access.

147. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

148. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants owed duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information

from theft. Welltok's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

149. Defendants had duties to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

150. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

151. For instance, HIPAA required Welltok to notify victims of the Breach within 60 days of the discovery of the Data Breach. Welltok did not begin to notify Plaintiff or Class Members of the Data Breach on behalf of its Clients until October 31, 2023, and Plaintiff were not notified until December 4, 202, despite, upon information and belief, Welltok knowing on or before July 26, 2023, that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiff and the Class.

152. Defendants owed duties of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

153. Defendants' duties of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential Private Information, a necessary part of being employees and/or patients at Welltok's Clients.

154. Defendants' duties to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

155. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

156. Defendants also had duties to exercise appropriate clearinghouse practices to remove former employees' and patients' Private Information it was no longer required to retain pursuant to regulations.

157. Moreover, Defendants had duties to promptly and adequately notify Plaintiff and the Class of the Data Breach.

158. Defendants had and continue to have duties to adequately disclose that the Private Information of Plaintiff and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

159. Defendants breached their duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect

Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to audit, monitor, or ensure the integrity of their vendor's data security practices;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former employees' and patients' Private Information it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure their stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

160. Defendants violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

161. Plaintiff and Class Members were within the class of persons the Federal Trade

Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

162. Defendants' violation of Section 5 of the FTC Act and Welltok's violation of HIPAA constitutes negligence.

163. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

164. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

165. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the administrative services and software industries.

166. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

167. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems.

168. It was therefore foreseeable that the failure to adequately safeguard Class

Members' Private Information would result in one or more types of injuries to Class Members.

169. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

170. Defendants were in a superior position to prevent the Data Breach and to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

171. Defendants' duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

172. Welltok has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

173. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

174. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

175. As a direct and proximate result of Defendants' negligence, Plaintiff and other Class Members have suffered actual harm in the form of experiencing specific acts of fraudulent

activity and other attempts of fraud that required Plaintiff's efforts to prevent from succeeding.

176. Plaintiff and the Class have suffered and will continue to suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) general damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

177. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

178. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

179. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

180. Defendants' negligent conduct is ongoing, in that Defendants still hold the Private

Information of Plaintiff and Class Members in an unsafe and insecure manner.

181. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND CLAIM FOR RELIEF
NEGLIGENCE PER SE

(Brought by Plaintiff Weaver on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes [alternatively, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes] against Progress, Welltok, Virgin Pulse, and Corewell Health)

182. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

183. Plaintiff brings this claim against Progress, Welltok, Virgin Pulse, and Corewell Health on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes or, in the alternative, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes.

184. Defendants' duties arise from, inter alia, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

185. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure Private Information.

186. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' Private Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtain and store, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

187. Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence per se.

188. Plaintiff and Class Members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

189. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

190. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' Private Information to unauthorized individuals.

191. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendants' violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially

increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) lost value of their Private Information, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

THIRD CLAIM FOR RELIEF
INVASION OF PRIVACY (INTRUSION UPON SECLUSION)

(Brought by Plaintiff Weaver on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes [alternatively, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes] against Progress, Welltok, Virgin Pulse, and Corewell Health)

192. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

193. Plaintiff brings this claim against Progress, Welltok, Virgin Pulse, and Corewell Health on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes or, in the alternative, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes.

194. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information that Defendants failed to safeguard and allowed to be accessed by way of the Data Breach.

195. Defendants' conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

196. By intentionally and/or knowingly failing to keep Plaintiff's and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiff's and Class

Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

197. Defendants knew that an ordinary person in Plaintiff's and a Class Members' positions would consider Defendants' intentional actions highly offensive and objectionable.

198. Defendants invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

199. Defendants intentionally concealed from Plaintiff and class members an incident that misused and/or disclosed their Personal Information without their informed, voluntary, affirmative, and clear consent.

200. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendants' conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

201. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

202. As a direct and proximate result of the foregoing conduct, Plaintiff seek an award of damages on behalf of themselves and the Class.

FOURTH CLAIM FOR RELIEF
INVASION OF PRIVACY (PUBLIC DISCLOSURE OF PRIVATE FACTS)

(Brought by Plaintiff Weaver on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes [alternatively, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes] against Progress, Welltok, Virgin Pulse, and Corewell Health)

203. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

204. Plaintiff brings this claim against Progress, Welltok, Virgin Pulse, and Corewell Health on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes or, in the alternative, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes.

205. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information that they provided to Defendants, directly or indirectly, in exchange for Defendants' services, which Defendants mishandled and allowed to be comprised in the Data Breach.

206. As a result of Defendants' conduct, publicity was given to Plaintiff's and Class Members' Private Information, which necessarily includes matters concerning their private life.

207. A reasonable person of ordinary sensibilities would consider the publication of Plaintiff's and Class Members' Private Information to be highly offensive.

208. Plaintiff's and Class Members' Private Information is not of legitimate public

concern and should remain private.

209. As a direct and proximate result of Defendants' public disclosure of private facts, Plaintiff and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) lost value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

210. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

211. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, inter alia: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FIFTH CLAIM FOR RELIEF
BREACH OF AN IMPLIED CONTRACT

(Brought by Plaintiff Weaver on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes [alternatively, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes] against Progress, Welltok, Virgin Pulse, and Corewell Health)

212. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

213. Plaintiff brings this claim against Progress, Welltok, Virgin Pulse, and Corewell Health on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes or, in the alternative, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes.

214. Defendants required Plaintiff and Class Members to entrust it with their Private Information, directly or indirectly in connection with healthcare or health plan services provided to Plaintiff and Class Members.

215. In turn, and through internal policies set forth herein, Defendants agreed to safeguard and not disclose the Private Information they collect to unauthorized persons.

216. Plaintiff and the Class Members accepted Defendants' offer by providing Private Information to them in exchange for Defendants' services.

217. Implicit in the parties' agreement was that Defendants would adequately safeguard the Private Information entrusted to them and would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

218. Plaintiff and the Class Members would not have entrusted their Private Information to Defendants in the absence of such an agreement.

219. Defendants materially breached the contract(s) they had entered into with Plaintiff

and Class Members by failing to safeguard such Private Information and failing to notify them promptly of the intrusion into their computer systems that compromised such information. Defendants further breached the implied contracts with Plaintiff and Class Members by:

A. Failing to properly safeguard and protect Plaintiff and Class Members' Private Information;

B. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

C. Failing to ensure the confidentiality and integrity of electronic Private Information that Defendants created, received, maintained, and transmitted.

220. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Defendants' material breaches of their implied agreement(s).

221. Plaintiff and Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendants.

222. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

223. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

224. Defendants knew or should have known that Plaintiff and Class Members reasonably understood that Defendants would safeguard the Private Information Defendants

required Plaintiff and Class Members to disclose in order to provide healthcare and/or health plan services and communications to them through the Welltok platform used by Defendants. Despite Plaintiff's and Class Members' reasonable expectations, Defendants failed to implement appropriate cybersecurity protocols to protect the Private Information on their systems from the Data Breach.

225. In addition, Defendants failed to advise Plaintiff and Class Members of the Data Breach promptly and sufficiently, having waited at least three months to send Plaintiff and other Class Members a notice letter, notifying them of the Data Breach.

226. In these and other ways, Defendants violated their duties of good faith and fair dealing.

227. Plaintiff and Class Members have sustained injury and damages because of Defendants' breaches of their agreements, including breaches thereof through violations of the covenant of good faith and fair dealing, including, without limitation: including, without limitation: unauthorized disclosure of their Private Information and publication onto the dark web; monetary losses; lost time; anxiety, and emotional distress; loss of the opportunity to control how their Private Information is used; lost value of their Private Information; compromise and continuing publication of their Private Information; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen Private Information; continued risk to their Private Information, which remains in Defendants' possession and is

subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Private Information in their possession; increased risk of harm; and lost benefit of the bargain.

SIXTH CLAIM FOR RELIEF
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT

(Brought by Plaintiff Weaver on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes [alternatively, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes] against Progress, Welltok, Virgin Pulse, and Corewell Health)

228. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

229. Plaintiff brings this claim against Progress, Welltok, Virgin Pulse, and Corewell Health on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes or, in the alternative, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes.

230. Defendants entered into written contracts with Welltok's Clients, including Corewell Health, to provide contact-management platform services to their Clients.

231. In exchange, Defendants agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

232. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendants and Welltok's Clients. Defendants knew that, if it were to breach these contracts with its clients, the clients' patients and employees—Plaintiff and Class Members—would be harmed.

233. Defendants breached the contracts entered into with Welltok Clients by, among

other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiff and Class Members of the Data Breach.

234. Plaintiff and the Class were harmed by Defendants' breaches of contract with Welltok Clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

235. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

236. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

SEVENTH LAIM FOR RELIEF
UNJUST ENRICHMENT

(Brought by Plaintiff Weaver on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes [alternatively, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes] against Progress, Welltok, Virgin Pulse, and Corewell Health)

237. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

238. Plaintiff brings this claim against Progress, Welltok, Virgin Pulse, and Corewell Health on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes or, in the alternative, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes.

239. Defendants knew that Plaintiff and Class Members conferred a benefit upon them

and have accepted and retained that benefit by accepting and retaining the Private Information entrusted to them. Defendants profited from Plaintiff's retained data and commercialized and used Plaintiff's and Class Members' Private Information for business purposes.

240. Defendants failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

241. Defendants acquired the Private Information through inequitable means as they failed to disclose the inadequate data security practices previously alleged. If Plaintiff and Class Members had known that Defendant would not fund adequate data security practices, procedures, and protocols to sufficiently monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information to Defendants or obtained employment and/or healthcare services from Corewell Health.

242. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own benefit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security and the safety of their Private Information.

243. If Plaintiff and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information at Defendants

or obtained employment and/or healthcare services at Corewell Health.

244. Plaintiff and Class Members have no adequate remedy at law.

245. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon them.

246. As a direct and proximate result of Defendants' conduct, Plaintiff and other Class Members, have suffered actual harm in the form of experiencing specific acts of fraudulent activity and other attempts of fraud that required Plaintiff's efforts to prevent from succeeding.

247. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer additional injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

248. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

249. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

SEVENTH CLAIM FOR RELEIF
VIOLATION OF MASSACHUSETTS GENERAL LAWS, CHAPTER 93A

(Brought by Plaintiff Weaver on behalf of the Progress Nationwide Class against Progress)

250. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

251. Plaintiff brings this claim against Progress on behalf of the Progress Nationwide Class.

252. M.G.L. ch. 93A § 2 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." M.G.L. ch. 93A § 9 permits any consumer injured by a violation of M.G.L. ch. 93A § 2 to bring a civil action, including a class action, for damages and injunctive relief.

253. Plaintiff alleges that Defendant Progress committed unfair business acts and/or practices in violation of M.G.L. ch. 93A §§ 2 and 9.

254. Defendant Progress knew or should have known of the inherent risks in experiencing a data breach if Progress failed to maintain adequate systems and processes for keeping Plaintiff's and Progress Nationwide Class Members' Private Information safe and secure. Only Defendant Progress was in a position to ensure that its systems were sufficient to protect against harm to Plaintiff and Progress Nationwide Class resulting from a data security incident such as the Data Breach; instead, Progress failed to implement such safeguards.

255. Defendant Progress's own conduct also created a foreseeable risk of harm to Plaintiff and Progress Nationwide Class Members and their Private Information. Defendant

Progress's misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent the Data Breach.

256. Defendant Progress acknowledges its conduct created actual harm to Plaintiff and Class Members because Progress instructed them to monitor their accounts for fraudulent conduct and identity theft.

257. Defendant Progress knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting Private Information and the importance of adequate security because of, inter alia, the prevalence of data breaches.

258. Defendant Progress failed to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Plaintiff's and Progress Nationwide Class Members' Private Information, failed to recognize in a timely manner the Data Breach, and failed to notify Plaintiff and Progress Nationwide Class members in a timely manner that their Personal Information was accessed in the Data Breach.

259. These acts and practices are unfair in material respects, offend public policy, are immoral, unethical, oppressive, and unscrupulous and violate 201 CMR 17.00 and M.G.L. ch. 93A § 2.

260. As a direct and proximate result of Defendant Progress's unfair acts and practices, Plaintiff Weaver and the Progress Nationwide Class have suffered injury and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and/or fraudulent use of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate

the actual and future consequences of Defendants' Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Defendants' possession (and/or to which Defendants continue to have access) and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed Private Information.

261. Neither Plaintiff nor the other Progress Nationwide Class Members contributed to Defendants' Data Breach.

262. Plaintiff sent a demand for relief, in writing, to Progress on June 12, 2024, prior to filing this complaint, as required by M.G.L. c. 93A § 9. Plaintiff has not received a written tender of settlement that is reasonable in relation to the injury actually suffered by Plaintiff and the Progress Nationwide Class.

263. Based on the foregoing, Plaintiff and the Progress Nationwide Class Members are entitled to all remedies available pursuant to M.G.L ch. 93A, including, but not limited to, refunds, actual damages, or statutory damages in the amount of twenty-five dollars per violation, whichever is greater, double or treble damages, attorneys' fees and other reasonable costs.

264. Pursuant to M.G.L. ch. 231, § 6B, Plaintiff and other members of the Progress Nationwide Class are further entitled to pre-judgment interest as a direct and proximate result of Defendants' wrongful conduct. The amount of damages suffered as a result is a sum certain and

capable of calculation and Plaintiff and other members of the Progress Nationwide Class are entitled to interest in an amount according to proof.

EIGHTH CLAIM FOR RELIEF
Violation of the Michigan Identity Theft Protection Act
Mich. Comp. Laws Ann. § 445.72, *et seq.*

(Brought by Plaintiff Weaver on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes [alternatively, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes] against Progress, Welltok, Virgin Pulse, and Corewell Health)

265. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein

266. Plaintiff brings this claim against Progress, Welltok, Virgin Pulse, and Corewell Health on behalf of the Progress, Welltok, Virgin Pulse, and Corewell Health Nationwide Classes or, in the alternative, the Progress, Welltok, Virgin Pulse, and Corewell Health State Classes.

267. Defendants are businesses that own or license computerized data that includes PII as defined by Mich. Comp. Laws Ann. § 445.72(1).

268. Plaintiff Weaver's and Class Members' personal information (for the purpose of this count, "PII"), (e.g., Social Security numbers) includes PII as covered under Mich. Comp. Laws Ann. § 445.72(1).

269. Defendants are required to accurately notify Plaintiff and Class Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

270. Because Defendants discovered a security breach and had notice of a security breach, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

271. It took Defendants approximately four months to send Notice Letters to Plaintiff Weaver and other Class Members, notifying them of the Data Breach, after Welltok and Virgin Pulse had been alerted of it.

272. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Mich. Comp. Laws Ann. § 445.72(4).

273. As a direct and proximate result of Defendants' violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Class Members suffered damages, as described above.

274. Plaintiff and Class Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

NINTH CLAIM FOR RELIEF
DECLARATORY RELIEF
(28 U.S.C. § 2201)

(Brought by Plaintiff Weaver on behalf of the Nationwide Class against All Defendants)

275. Plaintiff re-alleges and incorporates by reference all preceding paragraphs, as if fully set forth herein.

276. An actual controversy has arisen and exists between Plaintiff and Class Members, on the one hand, and Defendants on the other hand, concerning the Data Breach and Defendants' failure to protect Plaintiff's and Class Members' Private Information, including with respect to the issue of whether Defendants took adequate measures to protect that information. Plaintiff and the Class are entitled to judicial determination as to whether Defendants have performed and are adhering to all data privacy obligations as required by law or otherwise to protect Plaintiff's and Class Members' Private Information from unauthorized access, disclosure, and use.

277. A judicial determination of the rights and responsibilities of the parties regarding Defendants' privacy policies and whether they failed to adequately protect Private Information is

necessary and appropriate to determine with certainty the rights of Plaintiff and the Class, and so that there is clarity between the parties as to Defendants' data security obligations with respect to Private Information going forward, in view of the ongoing relationships between the parties.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as Class Representative and undersigned counsel as Class Counsel;

B. Find in favor of Plaintiff and the Class on all counts asserted herein;

C. Award Plaintiff and the Class monetary damages, including actual and statutory, compensatory damages, consequential, nominal, and punitive damages, to the maximum extent as allowed by law;

D. Award compensatory, consequential, general, and nominal damages in an amount to be proven at trial;

E. Award restitution and all other forms of equitable monetary relief;

F. Award equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein regarding to the misuse or disclosure of the private information of Plaintiff and Class members, and from refusing to issue prompt, complete, and accurate disclosure to Plaintiff and Class members;

G. Award injunctive relief as permitted by law or equity to assure that Class members have an effective remedy, and to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

ii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

iii. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the private information of Plaintiff and Class members;

iv. prohibiting Defendants from maintaining the private information of Plaintiff and Class members on a cloud-based database;

v. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

viii. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

ix. requiring Defendants to conduct regular database scanning and securing checks;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate;

xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers;

xvi. requiring, for a period of 10 years, the appointment of a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xvii. requiring Defendants to implement multi-factor authentication requirements, if not already implemented;

xviii. requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices.

H. Award disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts;

I. Award a mandatory injunction requiring that Defendants provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII and PHI to unauthorized persons.

J. Order Defendants to purchase or provide funds for lifetime credit monitoring and identify theft insurance to Plaintiff and Class members;

K. Order Defendants to pay the costs in notifying Class members about the judgment and administering the claims process.

L. Award Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowed by law;

M. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial;

N. Award Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable;

O. Distribute any monies recovered on behalf of members of the class or the general public via fluid recovery or cy pres recovery where necessary and as applicable to prevent Defendant from retaining benefits of their wrongful conduct;

P. Award Plaintiff and the Class such other favorable relief as allowable under law or at equity; and

Q. Award such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: June 20, 2024

Respectfully submitted,

/s/ Kristen A. Johnson

Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Plaintiff's Liaison & Coordinating Counsel

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Gary F. Lynch

LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com

Plaintiff's Lead Counsel

Joseph M. Lyon
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Jeffrey S. Goldenberg (Ohio #0063771)
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Phone: (513) 345-8291
Fax: (513) 345-8294
jgoldenberg@gs-legal.com

Steve W. Berman
Sean R. Matt
HAGENS BERMAN SOBOL SHAPIRO
1301 Second Avenue, Suite 2000
Seattle, WA 98101
Phone: (206) 623-7292
Fax: (206) 623-0594
steve@hbsslaw.com
sean@hbsslaw.com

Additional Counsel for Plaintiff Weaver

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was served by filing it on the Court's CM/ECF system, which will automatically send a notification of such filing to all counsel of record via electronic mail.

Dated: June 20, 2024

/s/ Kristen Johnson
Kristen Johnson